張貼日期：2022/07/11

【攻擊活動訊息QNAP 提醒用戶近期出現針對使用者密碼強度不足的裝置發動之 Checkmate 勒贖攻擊

- 主旨說明QNAP 提醒用戶近期出現針對使用者密碼強度不足的裝置發動之 Checkmate 勒贖攻擊

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心(TWCERT/CC)
  - 在 QNAP 發表的資安通報中指出Checkmate 勒贖攻擊主要針對【使用者密碼強度不足】，開啟了 SMB Windows 檔案分享服務，且裝置直接連上 Internet 的 NAS 裝置，發動字典檔暴力試誤登入攻擊；如果裝置使用預設登入帳號與弱密碼，就很可能遭到駭侵者成功登入，並將裝置上的檔案進行加密。
- 影響平台：\\開啟SMB Windows 檔案分享服務，且裝置直接連上 Internet 的 NAS 裝置。
- 建議措施：
  1. 避免直接讓裝置的 SMB 服務在外部 Internet 上曝露；如需自外網連線裝置的 SMB 協定，可參照該公司提供的操作指南，透過 VPN 連線來進行資料存取。
  2. 停用 SMB
  3. 將使用中的 QNAP 裝置更新到最新版 QNAP 作業系統。
  4. 立即審視所有 NAS 上的使用者帳號，確認密碼強度足夠。
  5. 定期備份檔案並執行檔案快照作業。
  6. 將系統預設的 admin 帳號停用，改用其他不容易被猜到的帳號設定為系統管理員專用帳號。
  7. 在系統防火牆中設定規則，將多次嘗試登入失敗的 IP 列入黑名單，禁止再次連線。
- 參考資料：
  1. https://www.qnap.com/en/security-advisory/qsa-22-21
  2. https://www.bleepingcomputer.com/news/security/qnap-warns-of-new-checkmate-ransomware-targeting-nas-devices/
  3. https://www.twcert.org.tw/tw/cp-104-6278-31aa8-1.html

計算機與通訊中心
網路系統組 敬啟